Application of the "Inherently Safer Technology (IST)" Concept to the Challenge of Security Risk Management

Lawrence M. Stanton, Senior Technical Advisor
Office of Infrastructure Protection
National Programs & Protection Directorate
U.S. Department of Homeland Security

2010 Chemical Sector Coordinating Council Security Summit July 8, 2010

Homeland Security

Why IST and Why Now?

- Section 550 of the DHS Appropriations Act of 2007 gave the Department authority to regulate the security of “high-risk” chemical facilities
- In response to that mandate, DHS promulgated the Chemical Facility Anti-Terrorism Standards, or CFATS Regulation
- CFATS requires regulated high-risk chemical facilities to institute a security risk management program that meets prescribed performance standards
- DHS is proscribed by statute from requiring particular measures:

“Provided further, That the Secretary may not disapprove a site security plan submitted under this section based on the presence or absence of a particular security measure…”

Homeland Security

IST Within CFATS

- The CFATS Regulation is silent on the concept of IST
- Facilities are not required under CFATS to consider any IST-type options as part of their security risk management strategy
- Facilities are not proscribed from doing so either…

Homeland Security

"IST" is in the "DNA" of CFATS

- The CFATS Regulation is constructed to encourage the application of IST-like measures to the question of security risk management
  - The Top-Screen process hinges on the possession of specific chemicals in threshold quantities
  - In some cases, those chemicals have concentration levels associated with them
  - "Material changes" are reportable and DHS will re-consider tier level based on material changes
  - Hence, a facility can reduce or eliminate its CFATS risk tier level by changing its chemical holdings
  - A company with multiple facilities also has the option to consolidate operations involving certain chemicals

- **However…**

Homeland Security

IST and Security

- IST is a conceptual approach to SAFETY
- Safety and security are related, but they are not the same
- '*Inherently Safer*' measures are not necessarily more secure
- Measures which improve the inherent level of security may compromise safety in some cases
- Avoiding the 'shifting of risk' is a significant challenge

Homeland Security

The Challenges of IST

- **From the Government Perspective:**
  - IST is a concept which can and should serve as a model for one of the tools we use in reducing national security risk
  - IST approaches should be considered with a national security risk perspective, and not solely from the point of view of individual companies/facilities
  - As with any regulatory element, outcomes of any IST-type initiative must be reasonably predictable, measurable, and manageable
  - The Department recognizes the complexity inherent in all questions of risk balancing

- **From the Industry Perspective:**
  - "IST" is a concept, not a list of some kind. Hence, "*consideration*" becomes an open-ended proposition limited only by the imagination
  - IST decisions are often about choosing which risks to accept and which to eliminate or reduce – the decision process is rarely "black and white"
  - The safety and engineering communities are made uneasy by the prospect of government officials substituting their judgment for the judgment of industry professionals in questions of risk balancing

Homeland Security

Today's Discussion

- Let's postulate that any "IST Option" could include any or all of the following:
  - A requirement to "***Consider***" IST-style measures that may impact a facility's security risk level and so contribute to the security risk management program
  - A requirement to "***Document***" that consideration, including what measure was considered, what factors were assessed in determining its desirability, and what was the result of that consideration
  - A requirement to "***Report***" that deliberative process and provide the documentation to DHS
  - A requirement to "***Implement***" those measures that meet a certain practicality test, or which are ordered by DHS to be implemented

Homeland Security

How ISCD Calculates Security Risk to Chemical Facilities

- In order to place chemical facilities into different tier levels, we have to calculate risk using a number of factors. These are:
  - Consequence, or "C": We estimate how severe the impact of a successful terrorist attack on a facility could be

    The primary consideration for security risk is "Consequence"

  - Threat, or "T": We estimate the level of static threat (national level terrorism) to a facility in a given location

    Facilities are unable to influence "Threat"

  - Vulnerability, or "V" – We estimate the relative difficulty a terrorist would have in producing the worst consequence by attacking the facility

    Facilities should account for all security risk reduction measures used to reduce "Vulnerability"

Homeland Security

The Equation

- This is (roughly) the equation we use in determining the security risk present at a given chemical facility:

$$C_3 \cdot T \cdot V = R_S$$

  - Where C_3 is Consequence
  - Where T is Threat
  - Where V is Vulnerability
  - Where R_s is the Security Risk
- Where do we get these values?

Homeland Security

Consequence

- Except when estimating economic criticality, we measure consequence in terms of how many people are at significant risk of death. Consequence (or "C") values are objectively designed.
- Consequence is determined by:
  - What chemical is present and in what quantity
    - *How it is held (gas, liquid under pressure, etc.)*
    - *Size and distribution of vessels/containers*
    - *Portability and whether it is shipped off site*
  - Where and how many people are within the potential impact area for that chemical
  - If a portable container is stolen, how much material (the weapon) is available and what percentage of a notional population would be at significant risk of death
  - Lethal effects include toxicity, overpressure, and radiated heat

Homeland Security

Threat

- Threat is measured in terms of the facility's location
- "Threat" for the purpose of CFATS security planning is relatively static
  - We assume a baseline level of capability of the adversary
  - We update/adjust for information in the intelligence stream periodically
  - The factors that go into a static "Threat" value are geospatial;
    - *Proximity to an international border or littoral*
    - *Past acts or attempted acts of national level terrorism in the State or an adjoining State*
    - *Population density*
    - *Infrastructure density*
    - *Coincidence of population density and infrastructure density*
    - *A factor derived from threat stream data assigned at the State level*

Homeland Security

Vulnerability

- Vulnerability is measured by accumulating “scores” or weights for any and all security risk management measures that a facility has in place or is scheduled to install/implement
- Each such measure has a value that can vary by:
  - The attack type being considered
  - The “target” being protected
  - The presence or absence of another measure
    - *One type of measure may negatively affect the value of other measures. (e.g. A security patrol is worth less if the facility lacks adequate lighting).*

Homeland Security

Security Risk (R_S)

- We calculate the potential c*onsequence* of a successful terrorist attack on a facility
- We calculate the level of *threat* to that facility based on its location
- We calculate how *vulnerable* the facility is to attack
- We give significant weight to the consequences
- We use these factors to determine a level of *Security Risk*
- We also know, as part of our process, WHY a facility is “high risk”
- We then communicate the LEVEL of security risk (Tier) and WHY the facility is high-risk (Risk Issue) to the facility (Final Tier Letter)

$$C_3 \cdot T \cdot V = R_S$$

Homeland Security

So What is Happening Now?

- Because the CFATS rule incentivizes facilities to reduce consequences, many facilities have made changes to their chemical holdings
- In many cases, these changes reflect application of the IST concepts of reducing or substituting chemicals
  - Sufficient documentation is needed to ensure DHS that these changes are not shifting security risk from one place or community to another
- DHS believes the CFATS rule is already having an “IST Effect”
  - The “IST effect” is not always well managed and may not be reducing the nation’s overall security risks
- Therefore, we are working to develop a new approach that could be utilized *regardless* of whether legislation to require IST implementation is enacted
  - By starting the process and research now, we can adapt implementation to reflect a mandate from Congress if and when that decision is made

Homeland Security

The First Issue

- DHS believes a program facilitating the consideration of IST approaches to security risk management is practically achievable and should be used where practicable
- The first issue we would hope to see addressed is that of terminology and definition
- “IST” is a safety discipline, not a security discipline
- The Department of Homeland Security regulation is focused on mitigating security risk
- The Department is evaluating IST with a focus on whether or when the adoption of an IST solution would reduce security risks

Homeland Security

Consider, Document and Report

- A structured program to "*Consider, Document and Report (CDR)*" IST type options would allow DHS to begin understanding the options and processes in context
  - The CDR element could be made part of the SSP submission, incorporated under the "proposed measures" section
  - The CDR element might be to evaluate a defined range of possibilities, and to do so against a defined set of considerations
  - If there were a defined scope for evaluation, and then a defined range of what must be considered in determining if an evaluated approach is viable, we could overcome the open-endedness issue and narrow the focus of our efforts to those IST-type options providing a significant risk-reduction benefit
  - Information submitted to DHS is already protected under Chemical Terrorism Vulnerability Information (CVI), which allows access to sensitive data only to those who have a need to know and who are authorized CVI users

Homeland Security

Even Today, IST-Type Options Can be "Proposed" to DHS

- IST-type measures can be included under the "proposed measures" component of the SSP
- IST-type options can be a powerful component of a security risk management program and expressed in the SSP
- Such options considered under the SSP may be options the facility wants to implement. DHS would be able to weigh in prior to implementation for two reasons:
  - *We can evaluate whether the proposed IST option would affect the facility's security risk before substantive resources are committed to the project*
  - *We will evaluate whether the proposed IST option would reduce overall risk, or simply shift that risk to a different community*

Homeland Security

The Key Test – Is Risk Really Reduced?

- For DHS, the key consideration in deciding to implement (or not implement) an IST-type option is this:

Does the option actually reduce security risk, or does the option simply change the risk without yielding any actual reduction?

- In many cases, an IST-type option will affect security risk but will not actually reduce security risk. (This challenge also exists in the implementation of Inherently Safer Technologies in relation to safety)
- The last test of an option, then, is to decide if risk is really reduced or not. DHS uses an approach like this:

Security Risk Tradeoff Analysis				
Compared to the Target Risk, the Countervailing Risk affects:	*Compared to the Target Security Risk, the Countervailing Security Risk is:*			
		Same Type	Different Type	Lesser Type
	Same Population	Risk Offset	Risk Substitution	Risk Reduction
	Diferent Population	Risk Transfer	Risk Transformation	Risk Reduction
	Less Population	Risk Reduction	Risk Reduction	Risk Reduction

Homeland Security

The Bottom Line

- DHS believes that the safety and engineering communities can assist the Department in identifying a reasonable scope for what must be considered, thus solving the open-endedness problem
- DHS believes a systematic approach to the consideration of IST-type options would yield some eye-opening findings and could materially reduce security risk in the Homeland

Homeland Security

Contact Information

- **Snail Mail:**

  Lawrence M. Stanton, Senior Technical Advisor
  Office of Infrastructure Protection
  National Programs & Protection Directorate
  U.S. Department of Homeland Security Mail Stop 8100

- **Email: Lawrence.Stanton@dhs.gov**

Homeland Security

CFATS Help Desk Contact Information

- The CFATS Help Desk toll-free number is 1-866-323-2957
  - Hours of Operation are 7:00AM – 7:00PM, Monday through Friday
  - The Help Desk is closed for Federal Holidays
- The CFATS Help Desk email address is CSAT@DHS.gov
- For CFATS Frequently Asked Questions (FAQ), regulation and guidance documents, and CVI training go to:
  WWW.DHS.GOV/CHEMICALSECURITY

Homeland Security